UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,406	12/29/2003	Bo-Heung Chung	51876P554	7550

8791 7590 10/19/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER
PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
10/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

80

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/748,406	CHUNG ET AL.	
	Examiner	**Art Unit**	
	Yogesh Paliwal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 10 August 2007.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-10 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-10 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on August 10, 2007 has been entered. Applicant has amended claims 1, 2, 5, 6, 7, and 10. Currently claim 1-10 are pending in this application.
- Examiner acknowledges receiving a replacement specification paragraph 0053 that is amended to correct typographical error. As a result, objection on the specification is withdrawn.
- Examiner acknowledges amendment for claims 2 and 7 to overcome 35 U.S.C. 112 second paragraph rejection. Applicant has successfully overcome the rejection with this amendment. As a result, 35 U.S.C 112 second paragraph rejection of claims 2 and 7 is withdrawn.

Response to Arguments

1. Applicant's arguments filed on Aug 10, 2007 have been fully considered but they are not persuasive for the following reasons:

    - Applicant argues that: "However, Matron does not disclose the generation of a replica of the old program before the switchover operation. In Figure 1 of Matron, program A and program B are two different old programs, and program A' and program B' are two different new programs. Marron does not disclose generating a replica of any of the new or old programs. Further, the switchover operation disclosed by Marron does not involve changing the replica of any of the programs".

- In reply, examiner would like to point to Column 2, lines 67-68, and Column 3, lines 1-6, which recites *"The running code (the old version which is being changed) should not have required or otherwise undergone a restructure, a requite or other modification in order to position it for the dynamic change at hand. An "ordinary" change should be applied to "ordinary" and existing code with the help of an external facility, and with the help of an administrative process"*. This part clearly recite that the old code that is running within the kernel should not be updated and existing code (witch is a copy) is used for updating the old code. Also as previously pointed by examiner at column 6, lines 50-53 which recites *"Prior to activation of the DSUF, the new programs are created by a change programmer modifying the old programs, recompiling, and linking the new programs to form load modules 23 and 25"*. Since the system of Marron requires the old code and the new code to co-exist for sometime before the switchover can happen, it is clear that the update is not being done on the old code which is already running in the kernel, and infect are done on the copy of an old code with the help of change programmer modifying the old programs, as recited at Column 6, lines 50-53. Also at column 3, lines 38-42, Marron clearly discloses running a code and a copy of the code at the same time and then updating the "idle copy" and then perform a switchover is well-known (see column 3, lines 38-42, *"Initially, all the transactions are processed by one copy of the transaction processing system (TPS) while the other copy is idle. The change is implemented on the* *idle copy of the TPS which in turns begins to process all newly arriving transactions".*) Therefore, examiner disagree with applicant that "Marron does not disclose generating a replica of any of the new or old programs code" and as pointed out at various places in Marron references (Specifically at Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42), it is now clear that Marron discloses generating a replica or a copy of an old program and updating it according to a change information.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

<u>Claims 1-4, 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron (US 5359730) in view of Ko (US 7024694)</u>

Regarding **Claims 1 and 6**, Marron discloses method and the inherent corresponding computer program for dynamically changing software module in a kernel level, the method comprising the steps of:

a) generating a replica of the old program in a kernel area **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42, for detailed explanation, refer to "Response to Arguments" section);**

b) changing the replica of the old program into a new program in response to a request from a user area for updating the old program. **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42, for detailed explanation, refer to "Response to Arguments" section)**; and

c) changing a currently applied program by exchanging a value of a pointer representing the old program with a value of a pointer representing the new program. **(Column 8, lines 49-52)**

Marron discloses a method of dynamically making software changes in a running system, however he does not teach dynamically changing an intrusion detection rule in a running system.

However, Ko, in the same field of endeavor of intrusion detection at kernel level, discloses that kernel level intrusion detection was well known in the art at the time applicant's invention was made (Column 1, lines 16-21)

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to apply the method of Marron to dynamically update kernel level intrusion detection rules of Ko *to non-disruptively install new versions of operating system [intrusion detection rules] modules while the system is running and one or more processes are executing which use and access such modules* (Marron, Column 5, lines 25-55)

Regarding **Claims 2 and 7**, the rejection of claims 1 and 6 is incorporated and further combination of Marron and Ko discloses a step of generating a replica of the new program [currently applied updated software] **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42,** Since Marron system require to do any update on a running code to be first performed on a copy of the code, it is implied that for performing any future update on the newly applied code, it would generate another copy and repeat the same process again to update currently new code to reflect any future updates**)**

Regarding **Claims 3 and 8**, the rejection of claims 1 and 6 is incorporated and further Marron discloses in the step b) and the step c), a change state of the intrusion detection rule [software] with a pre-assigned global variable is shown and the intrusion detection rule [software] is changed according to the pre-assigned global variable **(Marron, Column 5, lines 35-41)**

Regarding **Claims 4 and 9**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Ko discloses that the kernel area transfers the request of changing the intrusion detection rule [updating the software] from the user area by using a system call **(Marron, Column 7, lines 25-28)**

Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron (US 5359730) and further in view of Stoica (PHD thesis, "Stateless Core: A scalable Approach for Quality of Service in the Internet, Publication date: 12/15/2000)

Regarding **Claims 5 and 10**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Ko discloses that the kernel area transfers the intrusion detection result **(Ko, Fig. 1, Numeral 105)** to an application program of a host, the intrusion detection rule being applied to the intrusion detection result **(Ko, Column 2, lines 16-20).**

The combination of Marron and Ko does not discloses that the intrusion detection result being transferred by setting the global variables inside the kernel and determining the transferring position inside the kernel.

However, Stoica, in the same field of endeavor of kernel level monitoring system discloses that the kernel area transfers the kernel-monitoring log by setting the global variables inside the kernel and determining the transferring position inside the kernel **(Page 139, lines 19-21, "To minimize the monitoring overhead, we use the ip_output function call to send this information directly from kernel to an external monitoring machine.")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to send the intrusion detection results of the Marron and Ko combination from kernel to an external device by setting the global variables inside the kernel and determine the transferring position inside the kernel, as taught by Stoica, *to minimize the monitoring overhead and it also avoids unnecessary context switching between the kernel and the user level* **(Stoica, Page 139, lines 19-21)**

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
10/12/20007

IM VU
PATENT EXAMINE
GY CENTER 2100